Центральным в теории «безопасности» является понятие «угроза». **Угроза и опасность** - это совокупность условий и факторов, вызывающих нарушение нормального функционирования и развития человека и общества.

Если говорить научным языком, - современная **информационная среда** - то есть «совокупность источников информации, в которых «погружена» конкретная аудитория» [72] - может оказывать на объект, принимающий информацию (на реципиента) так называемое **информационное воздействие** - такой вид воздействия, при котором человек обращается к какому-либо источнику информации (например, к другому человеку) за сведениями о том, как следует поступать (или думать) [72]. То есть, проще говоря, в поведении героя художественного фильма (или героя печатного художественного произведения) ребёнок может увидеть пример для подражания.

Воздействие это может носить опасный для формирующейся личности характер и трансформироваться в угрозы информационной безопасности детей. Проще говоря, пример для подражания может оказаться вредным.

Угрозами информационно-психологической безопасности детей является:

1. получение детьми непристойных (то есть не соответствующих принятым стандартам нравственности) материалов различного характера (например, порнографии, материалов, содержащих жестокость и ненормативную лексику, вульгарные или шокирующие выражения);

2. получение детьми материалов, в содержании которых отражается национальная или другая (например, религиозная, социальная) нетерпимость и пропаганда расового, национального и религиозного неравенства или антиобщественного поведения;

3. получение детьми материалов, содержащих рекламу и пропаганду опасной и вредной для здоровья человека продукции (например, алкоголя, табачных изделий, наркотических веществ).

Безопасность детей в сети Интернет

Современные дети и подростки, которых называют «цифровыми гражданами» легко осваивают компьютер, мобильные устройства и умело пользуются ими. При этом навыки детей в области безопасности в Интернете отстают от их способности осваивать новые приложения и устройства.

Основные опасности в Интернете для детей и подростков следующие:

1. Кибербуллинг (интернет-травля).

2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).

3. "Незнакомый друг" в социальных сетях.

4. Кибермошенничество.

5. Безопасность доступа в Сеть и кража личных данных техническими средствами.

6. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе.

7. Просмотр сайтов для взрослых.

Куда обращаться в случае интернет - угроз

Кроме правоохранительных организаций можно обратиться:

1. На **горячую линию «Дети онлайн»: 8–800–250–0015** (с 9 до 18 по рабочим дням, звонки по России бесплатные), e-mail:**helpline@detionline.com**. Это первый в России общественный проект, целями которого является консультирование и оказание психологической помощи детям и подросткам, столкнувшимся со сложностями во время коммуникаций в Интернете.

2. Родители (законные представители) несовершеннолетних могут обратиться в **Центр защиты детей от интернет-угроз** (ЦЗДИУ) через онлайн - форму. На сайте ЦЗДИУ указано, что Ваше обращение будет рассмотрено в течении 24 часов.

Также сообщается, что Центр работает не только на профилактику, но и на пресечение IT-угроз. Избранное направление деятельности не имеет аналогов, что подтверждается мнением ведущих специалистов и СМИ.

Номер телефона 8 (930) 888-65-15, в будние дни с 09:00 до 18:00 (не указано, что звонок бесплатный - ред.).

3. На **Горячую линию Региональной общественной организации «Центр Интернет-технологий»** (РОЦИТ). Заполните заявку, приложите нужные ссылки и документы. С вами свяжутся в течение трех дней. Специалисты Горячей линии проконсультируют вас и при необходимости свяжутся с профильными организациями и госорганами, которые могут решить проблему.

4. Подать сообщение в Роскомнадзор о ресурсе, содержащем запрещенную информацию.

5. Оставить свое сообщение о противоправном Интернет-контенте на сайте Лиги безопасного интернета.

1. Кибербуллинг (интернет-травля)

Это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить кибербуллинг (другое название - троллинг) могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

«Троллинг» может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В интернете, как правило, ребенок находится один на один с потенциальным обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло.

Фейсбук дает следующее определение кибербуллинга: "Травля может происходить где угодно и принимать различные формы — от распространения слухов и размещения нежелательных фото до угроз в чей-то адрес. Под травлей понимается умышленное оскорбление, запугивание и угнетение состояния других людей."

Почти половина российских подростков в 2017 году столкнулась с кибербуллингом, заявил глава Регионального общественного центра интернет-технологий (РОЦИТ) Сергей Гребенников. Об этом сообщает РИА Новости.

Согласно данным, приведенным на международном форуме по кибербезопасности Cyber Security Forum 2018 (CSF 2018), 48% подростков в возрасте 14-17 лет становились жертвами груминга (шантажа), 46% подростков стали свидетелями агрессивного онлайн-поведения, 44% — получали агрессивные сообщения.

Основные мотивы киберагрессоров это развлечения (46%), власть (40%) и причинение вреда другому и всплеск негатива (35%), отмечается в материалах. При этом, только 17% детей обращаются за помощью к родителям.

Заведующий кафедрой новых медиа и теории коммуникации МГУ им. М.В. Ломоносова Иван Засурский, в мае 2016 года, выразил уверенность, что больше всего на юную психику влияет не тот или иной «взрослый» контент, к которому подросток всегда при желании получит доступ, а кибербуллинг. Явление, о котором в России начали говорить не так давно и опасность которого по-прежнему недооценивается.

«Не надо думать, что существуют какие-то отдельные онлайн-проблемы. Есть подростки, которых никто не воспитывает. Основная угроза для детей — это другие дети. Они бывают очень жестоки», — заявил Засурский.

Психологи и эксперты уверены: важно не следить за каждым шагом ребенка в интернете (зачастую это просто невозможно), а говорить с ним. «Как и в реальном, офлайновом мире, родителям не следует умалчивать о рисках использования интернета, равно как и о его возможностях и безусловной пользе в жизни каждого человека», — считает Денис Жилин из «Разумного интернета».

По мнению эксперта «Лаборатории Касперского», борьба с кибертравлей технически не так проста, поэтому и программный родительский контроль не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются за помощью к взрослым, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Поэтому **самую важную роль в защите ребенка от кибер-террора играют отношения с родителями**.

Старший научный сотрудник ESET, Дэвид Харли советует родителям пользоваться интернетом и, в частности, соцсетями вместе со своими детьми, начиная с дошкольного возраста. Это наиболее тактичный способ познакомить их с основами онлайн-безопасности.

2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).

Руководитель Центра защиты детей от интернет-угроз Владимир Рогов на вопросы Рамблер, 17.02.2018, в частности, сказал следующее:

- Считаю, что основной интернет-угрозой является **манипулятивно-идеологическая вербовка детей в различные движения**. Представьте классическую секту, но в соцсетях бывают более изощрённые направления, но смысл тот же — оторвать ребёнка от своего окружения (родители, друзья), приманить к себе, переделать в новый формат.

Также беспокоит напитка молодёжи контентом, который деформирует традиционные российские духовно-нравственные ценности, в частности, антисемейная пропаганда. **Это промежуточные звенья цепи, которые доводят детей до «групп смерти» и направления в формате «колумбайн»**.

С влиянием закрытых групп в социальных сетях связан 1% суицидов несовершеннолетних в России. На первых местах другие причины - неразделенная любовь и конфликты в семье - по 30%. Об этом 30.03.2017 на 5-м Всероссийском форуме "Наши дети" в Петербурге рассказал замначальника главного управления по обеспечению охраны общественного порядка (ГУОООП) МВД России Вадим Гайдов.

Он отметил, что в 2016 году несовершеннолетним в РФ было совершено 720 суицидов, в 2015-м - 685. Об этом сообщает ТАСС.

Вместе с тем в министерстве признали, что **в настоящее время особо актуальной становится проблема защиты детей от информации, распространяемой в так называемых закрытых группах, провоцирующих детей на суицид**.

Ранее председатель Следственного комитета РФ Александр Бастрыкин сообщил, что сегодня **всё большую опасность стали представлять собой "игры на выживание" или**

"игры на вымирание", организованные в интернете создателями так называемых "групп смерти". "Каждый день сотрудниками Главного управления криминалистики Следственного комитета Российской Федерации выявляются все новые и новые сообщества, которые ставят своей целью уничтожение молодежи", - подчеркнул председатель СК.

Подробнее

---

3. "Незнакомый друг" в социальных сетях

Исследования показывают, что среди людей, которые заходят на страничку ребенка в соцсетях, каждый второй — это человек, которого он никогда в своей жизни не видел, рассказывает профессор кафедры психологии личности МГУ им. М. В. Ломоносова **Галина Солдатова**.

"На факультете психологии МГУ мы изучаем новый феномен под названием "незнакомый друг". Это очень большой риск, потому что за каждым из незнакомцев может стоять кто угодно... наши дети... совершенно отчаянно и бесстрашно встречаются с незнакомцами из соцсетей.

Они назначают свидания, ходят по указанным адресам и т. д. Возможно, за дверью их ждет друг на всю жизнь, но с тем же успехом там может оказаться и педофил. Об этом с детьми просто необходимо говорить. Важно, чтобы они ценили приватность своего пространства в интернете точно так же, как ценят приватность своего личного пространства дома...

Ребенок может передать незнакомцам свои персональные данные, поделиться номером кредитки мамы, может сфотографировать квартиру, сообщить адрес, показать интерьер и ценные вещи, рассказать, что семья уезжает в отпуск, и т. д. Нужна очень серьезная кооперация всей семьи, чтобы уяснить: все, что мы выкладываем в интернет, становится достоянием огромного круга людей, которые далеко не всегда дружелюбно настроены. Мы подготовили специальную книгу для педагогов с уроками для школьников по защите персональных данных. Она может быть полезна и для родителей."

4. Безопасность доступа в Сеть и кража личных данных техническими средствами.

Впервые за все пять лет работы горячей линии «Дети онлайн» на второе место по актуальности вышли вопросы обеспечения безопасного доступа в сеть и защиты от краж личных данных техническими средствами. В 2014 году каждый третий обратившийся сталкивался с блокировкой компьютеров и внедрением на них вредоносных программ и вирусов, а также взломами личных профилей в социальных сетях и блогах.

5. Кибермошеничество

Для кражи личной информации пользователя, применяются все более сложные фишинговые схемы, в том числе с использованием узнаваемых брендов. В 2013 году число обращений по данному вопросу достигло 19%. Чаще всего интернет-пользователи обращались на линию уже после столкновения с мошенниками, чтобы получить консультацию по дальнейшим действиям.

6. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе

В мае 2014 года Роскомнадзор выявил более 200 сайтов, распространяющих в открытом доступе персональные данные несовершеннолетних россиян и их родителей.

Сайты, разместившие персональную информацию о детях, как правило, принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов Российской Федерации.

Обнаруженные данные содержали списки воспитанников детских садов и интернатов, учеников школ, с указанием их ФИО, даты рождения, места проживания, а также сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан. Речь идет о многодетных семьях, матерях-одиночках, безработных родителях, детях сотрудников правоохранительных органов, детях судей, детях, оставшихся без попечения родителей. На сайте одного из образовательных учреждений был опубликован список детей, направляемых на психоневрологическую комиссию.

Как говорится в сообщении Роскомнадзора, "распространение в открытом доступе персональной информации несовершеннолетних может повлечь за собой неблагоприятные последствия для детей и их родителей, связанные с неправомерным посягательством на частную жизнь семьи, здоровье и половую неприкосновенность детей".

Эксперты очень высоко оценили сайт персональныеданные.дети, где в занимательной, красочной и очень доступной форме объясняется самое главное из того, что следует знать по этой теме. Лучшей защитой для ребенка будет владение информацией об опасностях, с которыми он может столкнуться в Интернете. Именно в целях информирования о правилах обработки данных был создан этот сайт, - рассказывает зам. руководителя Роскомнадзора Антонина Приезжева.

"Изначально подача сайта была рассчитана на любую целевую аудиторию: от детей до взрослого человека. Замечу, что материалы, тесты, размещенные на портале, можно использовать и в образовательных целях, например, на уроках по интернет-безопасности", - отметила А.Приезжева.

В 2016 году, по сравнению с 2015 годом, было выявлено значительно меньше фактов размещения на официальных сайтах различных учреждений персональных данных детей – прежде число таких случаев выходило за все разумные рамки и объемы.

7. Просмотр сайтов для взрослых

По результатам исследования «Лаборатории Касперского», из всех сайтов с маркировкой 18+ наибольший интерес для российских детей представляют эротические и порнографические сайты - 46,4%, на втором месте оружейная тематика - 26,4%, на третьем - нецензурная лексика - 10,7%.

Следует обратить внимание, что указанные проценты - это удельный вес не всех посещаемых несовершеннолетними сайтов, а только входящих в категорию нежелательных. Ещё точнее - в эти проценты вошли и неудачные попытки попасть на "взрослые" сайты, если они были заблокированы модулем «Родительский контроль».

Сам по себе результат исследования не очень интересен. Чего хочется большинству детей? Поскорее стать взрослыми. И любая маркировка "только для взрослых" еще больше разжигает интерес, считает психолог Елена Кузнецова.

Вывод исследования очевиден - **Безопасность ребенка в Сети = Контроль со стороны родителей + «Родительский контроль»**.

По данным Центра новостей ООН 92% родителей утверждают, что они установили четкие правила поведения для своих детей в Интернете. Однако, эти данные не совпадают с данными опроса детей. 34% детей заявили, что их родители не устанавливали никаких правил и не контролируют то, как они пользуются Всемирной паутиной.

85% родителей сказали, что слышали о программном обеспечении, позволяющем установить родительский контроль на компьютере, которым пользуется ребенок. Но только 30% родителей решили им воспользоваться.

В октябре 2013 года результаты исследования, проведенные Лигой безопасного интернета, МТС и "Лабораторией Касперского" показали, что в России только 21,5% родителей контролируют детей в возрасте от 6 до 17 лет, говоря, на какие сайты заходить можно или нельзя.

Одно из решений этой проблемы - включить опцию "родительский контроль", которая есть у всех антивирусов с Internet Security. Кроме этого, можно установить дополнительную программу. Разновидностей этих программ, по доступной всем цене, уже несколько десятков.

Возможно, кого-то заинтересует **KinderGate Родительский Контроль**. Эту программу от большинства подобных решений отличает следующее:

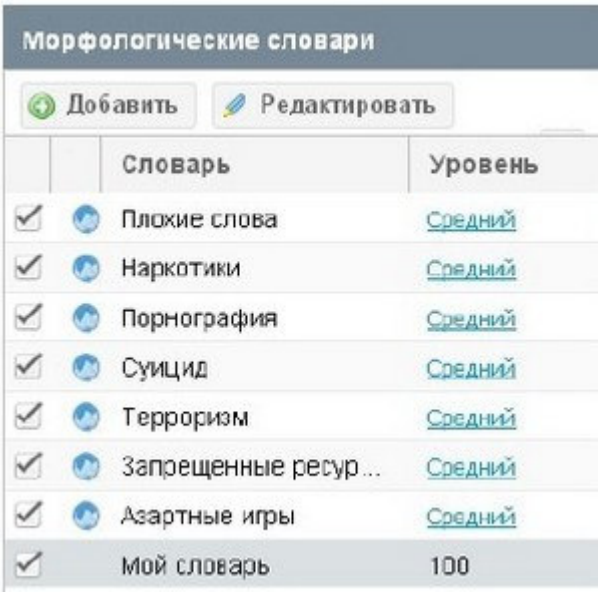
* невозможно отключить или удалить без знания пароля, заданного при установке;

* корректно работает совместно с любыми антивирусами, поддерживает Linux-системы и Mac OS;

* использует **ежедневно обновляемую базу из 500 миллионов сайтов**, когда как наборы интернет-ресурсов других решений насчитывают лишь 10-15 миллионов;

* обеспечивает дополнительный уровень защиты посредством инструмента морфологического анализа;

В KinderGate это можно сделать примерно так:



* можно контролировать скачивание определенных видов файлов (EXE, DOC, MP3, AVI, и т.д.);

* бесплатный тестовый период 30 дней.

Более подробная информация - на сайте KinderGate Родительский Контроль

Что делать если ребенок смотрит сайты для взрослых?

Например, на вопрос:"У меня сыну 12 лет, недавно обнаружила, что он смотрит порно, как быть, что делать?", - на сайте Liveexpert.ru был дан следующий ответ:

1. Включите на компе функцию «родительский контроль».

2. Купите и положите ему на стол книгу «Сексуальная энциклопедия для подростков». Это как минимум.

3. Скажите отцу (или дедушке) пусть поговорят с сыном о интересующих мальчика вопросах секса. Здесь не место ханжеству.

Психолог Елена Кузнецова по другому аналогичному вопросу на сайте All-psy.com советует следующее: "Ребенок найдет всю необходимую ему информацию - в интернете ли, от сверстников ли, но найдет обязательно. Так же как любые другие знания о жизни. Особенно заинтересованно будет искать, если почувствует, что родители ведут себя как-то странно: эмоционально подчеркивают особенность темы, называют "для взрослых". У большинства здоровых детей потребности в самих сексуальных отношениях еще нет. Ребенок просто интересуется сферой. Наиболее разумные родители снимают с темы ажиотаж."

Кстати, на указанных выше сайтах родители могут найти много полезной для себя информации или получить ответ на свой вопрос от квалифицированных психологов.

Простые советы компании ESET - "Как защитить ребенка в сети?"

- Создайте «детский» профиль пользователя на вашем ПК или ноутбуке, где будут лишь предназначенные для детей материалы (например, мультфильмы).
- Научите ребенка пользоваться социальными сетями и поисковыми сервисами. Заведите ему страничку в соцсетях и адрес электронной почты. Используйте разные пароли!
- Используйте настройки безопасности/приватности выбранных сайтов для ограничения доступа к личным данным вашего ребенка.
- Проверяйте возрастные ограничения сайтов и видеоигр. Многие из них не предназначены для несовершеннолетних.
- Объясните, что в интернете, как и в реальной жизни, не стоит общаться с незнакомыми людьми и тем более раскрывать информацию о себе или семье.
- Даже друзьям и знакомым не следует доверять на 100% – профиль одноклассника вашего ребенка может быть взломан злоумышленниками.
- Приглядывайте за тем, кого ваш ребенок добавляет в друзья в соцсетях и что публикует в открытом доступе.
- Если вашего ребенка в интернете кто-то напугал или расстроил – он должен знать, что в любой момент может прийти к вам и рассказать об этом.
- Убедитесь, что в вашей семье компьютеры, ноутбуки и мобильные устройства защищены антивирусным ПО. ESET NOD32 Smart Security Family для пяти устройств – оптимальный выбор.
- Активируйте в вашем антивирусном продукте функцию «Родительский контроль» и определите категории сайтов, которые необходимо блокировать (онлайн-магазины, казино, XXX-сайты и др).

http://www.bizhit.ru/

Концепция информационной безопасности детей

утверждена распоряжением Правительства РФ от 2 декабря 2015 года № 2471-р.

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи.

Необходима организация последовательных и регулярных мероприятий государства и общественных организаций, направленных на повышение уровня медиаграмотности детей, которые должны с раннего возраста приобретать навыки безопасного существования в современном информационном пространстве.

Усилия государства по ограничению доступа к ресурсам, содержащим противоправный контент, не смогут полностью оградить детей от вредной информации. Поэтому необходимо формировать у детей механизмы критической оценки получаемых сведений.

Также, необходимо продолжать работу по совершенствованию механизма блокировки сайтов в сети "Интернет", содержащих запрещенную информацию.

В интернет-зависимость уходит и множество морально покалеченных детей. Калечат их, к сожалению, сами родители. У таких детей нередко изрезаны руки, и это не обязательно суицид. Например, один мальчик, у которого были порезы от плеча до кисти, сказал на консультации: «Я не хотел себя убивать». Специалисту, конечно, понятно, что это некогда подавленная аутоагрессия.

Такая агрессивность начинает формироваться на втором этапе. Родители обычно еще не бьют тревогу, но уже делают замечания, а это приводит к сопротивлению и протесту детей. Внутри у ребенка накапливается очень много агрессии. Дети не могут выплеснуть ее на родителей, потому что это табуировано, но находят возможность вылить все это на кого-нибудь в интернете.

Не секрет, что подростки часто сами лишают себя возможности общаться вживую. А ведь это еще одна из социальных потребностей, закономерная для этого возраста: быть признанным противоположным полом.

В интернете же у них появляется возможность быть неким бесполым существом, которое всех и вся убивает, чувствуя себя сильным и крутым. Через такой суррогат удовлетворяются все потребности. Но это ужасно, потому что при этом полностью отсутствуют или игнорируются все социальные нормы и табу.

Если это впитается ребенком полностью, то из него просто-напросто вырастет преступник. В какой-то момент он подумает, что в реальной жизни тоже все дозволено. Один из таких ребят-игроманов на вопрос: «О чем ты тогда думал?» — ответил: «У меня было два желания — либо кого-то убить, либо чтобы меня убили» (к счастью, сейчас с этим мальчиком все хорошо). Вот результат интернет-игр и интернет-зависимости.

Интернет-зависимость — это чума XXI века. К сожалению, дети не способны справиться с этим сами. Я бы посоветовала родителям не конфликтовать с детьми, не отказываться от них, а принимать их такими, какие они есть.

Потому что доля участия родителей в том, что их ребенок стал таким, точно имеется. И утеря тех качеств, о которых мы говорили, происходит тоже благодаря им.

Здесь важно признать свои ошибки, но это сложнее всего — родители же всегда считают себя правыми.

Социолог и психолог Александр Журавль считает, что ошибочно полагать, что виртуальное пространство бесповоротно затуманило разум подростков и они готовы создать для него любой сюжет – даже самый жестокий. Об этом он рассказал за круглым столом: «В чем причина всплеска подростковой жестокости», который прошел 26.01.2016 в студии «Вечерняя Москва» (источник: Москва Центр).

Такое же мнение у Александра Ветушинского, научного сотрудника философского факультета МГУ, специалиста по теории видеоигр. — Сколько бы ни находилось случаев, когда можно сказать: «Мы нашли видеоигры у преступника дома, значит виноваты видеоигры, потому что они Простые советы компании ESET - "Как защитить ребенка в сети?"

- Создайте «детский» профиль пользователя на вашем ПК или ноутбуке, где будут лишь предназначенные для детей материалы (например, мультфильмы).
- Научите ребенка пользоваться социальными сетями и поисковыми сервисами. Заведите ему страничку в соцсетях и адрес электронной почты. Используйте разные пароли!
- Используйте настройки безопасности/приватности выбранных сайтов для ограничения доступа к личным данным вашего ребенка.

- Проверяйте возрастные ограничения сайтов и видеоигр. Многие из них не предназначены для несовершеннолетних.
- Объясните, что в интернете, как и в реальной жизни, не стоит общаться с незнакомыми людьми и тем более раскрывать информацию о себе или семье.
- Даже друзьям и знакомым не следует доверять на 100% – профиль одноклассника вашего ребенка может быть взломан злоумышленниками.
- Приглядывайте за тем, кого ваш ребенок добавляет в друзья в соцсетях и что публикует в открытом доступе.
- Если вашего ребенка в интернете кто-то напугал или расстроил – он должен знать, что в любой момент может прийти к вам и рассказать об этом.
- Убедитесь, что в вашей семье компьютеры, ноутбуки и мобильные устройства защищены антивирусным ПО. ESET NOD32 Smart Security Family для пяти устройств – оптимальный выбор.
- Активируйте в вашем антивирусном продукте функцию «Родительский контроль» и определите категории сайтов, которые необходимо блокировать (онлайн-магазины, казино, XXX-сайты и др).

жестоки», нельзя считать игры первопричиной. Видеоигры, конечно, могут быть причиной конкретного случая жестокости, но по большому счету такие случаи мне не попадались.

Важно не занятие ребенка, а его степень самоконтроля, ведь можно играть в Call of Duty, а можно читать Достоевского, и в каждом из случаев дети осознают, что реально, а что иллюзорно, — уверяет А.Ветушинский.

Безопасный интернет для детей

09.02.2017 в пресс-центре «Парламентской газеты» состоялся круглый стол, посвященный подведению итогов десятой «юбилейной» Недели Безопасного Рунета, мероприятия которой проходили в 60 регионах России с 31 января по 7 февраля 2017 года.

Количество детей, ежедневно пользующихся интернетом, выросло до 95%, привела данные профессор кафедры психологии личности МГУ Галина Солдатова: «При этом **32% детей сидят в сети каждый день по 8 часов**, хотя ещё три года назад их было всего 14%. На наших глазах формируется новое «цифровое» поколение, которое неизбежно сталкивается с рисками при пользовании Всемирной паутиной».

Домен .ДЕТИ – место, где ребенок находится в безопасности

16.06.2014 была открыта регистрация в новой доменной зоне .ДЕТИ, создание которой было инициировано Фондом "Разумный Интернет" с целью защитить детей и подростков от нежелательного контента и создать безопасное интернет-пространство для самых младших пользователей.

Новый кириллический домен верхнего уровня был создан при непосредственной поддержке Координационного центра национального домена сети Интернет. В сентябре 2015 года на пресс-конференции бывший директор Координационного центра Андрей Колесников подчеркнул, что борьба со всеми потенциальными опасностями интернета – это борьба с ветряными мельницами, и процесс этот требует очень много ресурсов.

«Поэтому мы решили создать маленький островок для детей – домен .ДЕТИ. У нас прагматичный подход: вместо того, чтобы строить преграды и фильтровать контент, мы создаем место, куда детей можно спокойно отпускать без надзора родителей и учителей. Мы гарантируем, что в этом домене (ред. bizhit.ru) ребенку не встретится неподходящая информация – за этим следят наши партнеры из «Спутника», с их помощью доменная зона .ДЕТИ ежесуточно проверяется на наличие небезопасного или вредного контента», - рассказал Андрей Колесников.

Домен объединяет сайты о детях и для детей с качественным и безопасным контентом. «**Если вы видите адрес в домене .ДЕТИ, знайте — это гарантия того, что пребывание детей и подростков на этом интернет-сайте будет комфортным и безопасным**», - утверждает Андрей Воробьев, директор Координационного центра.

07.02.2017 в Москве прошел международный форум по кибербезопасности – Cyber Security Forum 2017 (CSF 2017). В рамках секции «Контентная безопасность» выступил Денис Жилин, директор по маркетингу фонда «Разумный интернет». Он рассказал об опыте реализации системы мониторинга вредоносной активности на уровне домена .ДЕТИ:

«В зоне круглосуточно функционирует система мониторинга, которая позволяет определять так называемый "ненадлежащий контент". При обнаружении инцидентов служба реагирования получает отчет от автоматической системы, специалисты проверяют каждый такой случай и при подтверждении информации незамедлительно направляют владельцу ресурса уведомление с требованием устранить нарушение. На текущий момент **интернет-пространство, организованное с помощью .ДЕТИ, - одно из самых безопасных в мире**. Мы очень этим гордимся и призываем пользоваться возможностями домена всех, кто живет и работает на благо детей».

Специалисты, принимавшие участие в CSF 2017, также констатировали, что мы вступили в эпоху так называемого «цифрового детства»: информационно-коммуникационные технологии расширяют пространство жизнедеятельности ребенка и влияют на структуры его деятельности не только онлайн, но и офлайн.

Среди рисков, с которыми дети чаще всего сталкиваются в интернете, коммуникационные (35% случаев) и технологические (31%). Интересно, что столкнувшись с какой-либо проблемой в сети, за советом или решением юные пользователи предпочитают обращаться к учителям (в 15% случаев), нежели к родителям (8%).

Домен .ДЕТИ - это социальный проект, и его реализация не предполагает получения прибыли. По мнению учредителей, новая доменная зона позволит объединить профильные сайта и создать для детей полноценный сегмент интернета, адаптированный под подростковые интересы и способность восприятия.

«Большие проекты» в доменной зоне (сайты и порталы, название которых заканчивается на .дети):

1. КАРУСЕЛЬ
2. ТВОЕ
3. КАФЕ-АНДЕРСОН
4. РОСТЕЛЕКОМ
5. ГДЕ
6. ПЕРСОНАЛЬНЫЕДАННЫЕ
7. СПУТНИК
8. ВЕБ-ЛАНДИЯ
9. БИБЛИОТЕКА
10. КЛАССНЫЙ-ЖУРНАЛ
11. РАЗУМЕЙКИН
12. МАТЕМАТИКА-ПРОСТО
13. ПРОФЕССИИ
14. ЗДОРОВЫЕ

Источник: Домен .ДЕТИ

О проекте "Спутник.Дети"

На сайте проекта Спутник.Дети указано, что он сделан специально для детей. «Мы постарались наполнить его самыми лучшими и интересными сайтами для юных пользователей интернета и отобрали более 5000 сайтов: с мультфильмами, играми, раскрасками, книжками, песнями и многим другим. Даже школьные задачки мы постарались сделать нескучными.

Коллекция сайтов постоянно пополняется: этим каждый день занимаются наши роботы, а помогают им родители и сами ребята — ведь никто, кроме них, не сможет сказать лучше, какие игры, истории или мультики нравятся им больше всего.»

Директор поисковой системы "Спутник", Максим Хромов 06.11.2014 рассказал ИТАР-ТАСС о проекте "Спутник.Дети". «Это будет поисковый сервис специально для детей. Область поиска составит коллекция сайтов, зарегистрированных в доменной зоне .Дети, а также детские сайты, найденные в Рунете автоматическими поисковыми роботами и анализаторами "Спутника", и сайты, отобранные партнерами проекта.

Принять участие в развитии сервиса может любой владелец интернет-проекта для детей - достаточно предложить свой сайт на добавление в область поиска. Каждый ресурс проходит проверку асессорами поисковика и системой безопасности.

Сегодня в Рунете довольно серьезный дефицит качественных детских ресурсов - на них невелик спрос, потому что он формируется родителями и требует активной позиции, постоянного исследования вопроса, поиска новых сервисов и контента для ребенка.

В мае 2015 года на Большом Медиа-Коммуникационном Форуме, Денис Жилин (фонд "Разумный Интернет") в своем докладе сообщил, что под категорию "Дети и семья" (т.е. сайты, содержащие детский контент) в России подпадают всего 64 000 сайтов (это чуть больше одного процента от всего Рунета). К ядру наиболее посещаемых из них относятся 5 000 сайтов.

Быть хорошим родителем непросто в принципе, а в эпоху интернета еще сложнее: необходимо постоянно повышать свою квалификацию. Или пустить все на самотек в формате "ребенок чем-то занят в планшете - значит при деле". Наша задача повысить доступность качественного развивающего контента, а вместе с тем обозначить безопасную орбиту, внутри которой ребенок будет в безопасности», - объяснил Максим Хромов.

Директор "Спутника" считает, что мобильные устройства не мешают развитию детей. Более того, неправильно в мире современных технологий и гаджетов воспитывать ребенка в изоляции от них: в определенный момент он рискует оказаться отстающим. Все зависит от подхода к этому вопросу.

На вопрос: Как Вы считаете, кого на сегодняшний момент надо обучать правилам пользования интернетом - детей или сначала их родителей?

Максим Хромов ответил: « - Марк Твен, кажется, говорил: "Не воспитывайте детей, все равно они будут похожи на вас. Воспитывайте себя". Этой фразе больше ста лет, но, мне кажется, сейчас она не менее актуальна. Если взрослый человек не знает, как правильно пользоваться компьютером, интернетом, как он сможет помочь своему ребенку разобраться в том, какой контент вреден, а какой нет?

В определенный момент развития общества нормальной была ситуация, когда компьютер и интернет в семье появлялись только для ребенка, а родители не знали даже, как все это включается. Сегодня ситуация меняется. Только в семье и школе ребенок может получить представление о том, что такое хорошо, и что такое плохо в интернете, именно поэтому соответствующее представление о предмете должны быть в первую очередь у родителей и учителей.»

10 правил безопасности детей в интернете от Гугл

1. Поговорите с ребенком о безопасности в Интернете.Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите ребенка, что в любой непонятной или пугающей ситуации ему следует обращаться к родителям, чтобы найти безопасное решение.

2. Используйте компьютер и смартфон вместе с детьми. Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.

3. Расскажите детям больше о сайтах и сервисах в Интернете.Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.

4. Безопасные пароли. Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.

5. Используйте настройки конфиденциальности и управления доступом. В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.

6. Проверьте возрастные ограничения. Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок

зарегистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.

7. Научите детей ответственному поведению в Интернете. Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.

8. Посоветуйтесь с другими взрослыми. Привлеките к обсуждению этой темы друзей, родственников и педагогов. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь в том, как научить детей и родственников правильному использованию самых разных информационных технологий.

9. Защитите свой компьютер и личные данные. Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.

10. Не останавливайтесь на достигнутом. Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы.

Источник: Центр безопасности Google

Безопасный интернет для детей

09.02.2017 в пресс-центре «Парламентской газеты» состоялся круглый стол, посвященный подведению итогов десятой «юбилейной» Недели Безопасного Рунета, мероприятия которой проходили в 60 регионах России с 31 января по 7 февраля 2017 года.

Количество детей, ежедневно пользующихся интернетом, выросло до 95%, привела данные профессор кафедры психологии личности МГУ Галина Солдатова: «При этом **32% детей сидят в сети каждый день по 8 часов**, хотя ещё три года назад их было всего 14%. На наших глазах формируется новое «цифровое» поколение, которое неизбежно сталкивается с рисками при пользовании Всемирной паутиной».

Домен .ДЕТИ – место, где ребенок находится в безопасности

16.06.2014 была открыта регистрация в новой доменной зоне .ДЕТИ, создание которой было инициировано Фондом "Разумный Интернет" с целью защитить детей и подростков от нежелательного контента и создать безопасное интернет-пространство для самых младших пользователей.

Новый кириллический домен верхнего уровня был создан при непосредственной поддержке Координационного центра национального домена сети Интернет. В сентябре 2015 года на пресс-конференции бывший директор Координационного центра Андрей Колесников подчеркнул, что борьба со всеми потенциальными опасностями интернета – это борьба с ветряными мельницами, и процесс этот требует очень много ресурсов.

«Поэтому мы решили создать маленький островок для детей – домен .ДЕТИ. У нас прагматичный подход: вместо того, чтобы строить преграды и фильтровать контент, мы создаем место, куда детей можно спокойно отпускать без надзора родителей и учителей. Мы гарантируем, что в этом домене (ред. bizhit.ru) ребенку не встретится неподходящая информация – за этим следят наши партнеры из «Спутника», с их помощью доменная зона .ДЕТИ ежесуточно проверяется на наличие небезопасного или вредного контента», - рассказал Андрей Колесников.

Домен объединяет сайты о детях и для детей с качественным и безопасным контентом. «**Если вы видите адрес в домене .ДЕТИ, знайте — это гарантия того, что пребывание детей и подростков на этом интернет-сайте будет комфортным и безопасным**», - утверждает Андрей Воробьев, директор Координационного центра.

07.02.2017 в Москве прошел международный форум по кибербезопасности – Cyber Security Forum 2017 (CSF 2017). В рамках секции «Контентная безопасность» выступил Денис Жилин, директор по маркетингу фонда «Разумный интернет». Он рассказал об опыте реализации системы мониторинга вредоносной активности на уровне домена .ДЕТИ:

«В зоне круглосуточно функционирует система мониторинга, которая позволяет определять так называемый "ненадлежащий контент". При обнаружении инцидентов служба реагирования получает отчет от автоматической системы, специалисты проверяют каждый такой случай и при подтверждении информации незамедлительно направляют владельцу ресурса уведомление с требованием устранить нарушение. На текущий момент **интернет-пространство, организованное с помощью .ДЕТИ, - одно из самых безопасных в мире**. Мы очень этим гордимся и призываем пользоваться возможностями домена всех, кто живет и работает на благо детей».

Специалисты, принимавшие участие в CSF 2017, также констатировали, что мы вступили в эпоху так называемого «цифрового детства»: информационно-коммуникационные технологии расширяют пространство жизнедеятельности ребенка и влияют на структуры его деятельности не только онлайн, но и офлайн.

Среди рисков, с которыми дети чаще всего сталкиваются в интернете, коммуникационные (35% случаев) и технологические (31%). Интересно, что столкнувшись с какой-либо проблемой в сети, за советом или решением юные пользователи предпочитают обращаться к учителям (в 15% случаев), нежели к родителям (8%).

Домен .ДЕТИ - это социальный проект, и его реализация не предполагает получения прибыли. По мнению учредителей, новая доменная зона позволит объединить профильные сайта и создать для детей полноценный сегмент интернета, адаптированный под подростковые интересы и способность восприятия.

«Большие проекты» в доменной зоне (сайты и порталы, название которых заканчивается на .дети):

1. КАРУСЕЛЬ
2. ТВОЕ
3. КАФЕ-АНДЕРСОН
4. РОСТЕЛЕКОМ
5. ГДЕ
6. ПЕРСОНАЛЬНЫЕДАННЫЕ
7. СПУТНИК
8. ВЕБ-ЛАНДИЯ
9. БИБЛИОТЕКА
10. КЛАССНЫЙ-ЖУРНАЛ
11. РАЗУМЕЙКИН
12. МАТЕМАТИКА-ПРОСТО
13. ПРОФЕССИИ
14. ЗДОРОВЫЕ

Источник: Домен .ДЕТИ

О проекте "Спутник.Дети"

На сайте проекта Спутник.Дети указано, что он сделан специально для детей. «Мы постарались наполнить его самыми лучшими и интересными сайтами для юных пользователей интернета и отобрали более 5000 сайтов: с мультфильмами, играми, раскрасками, книжками, песнями и многим другим. Даже школьные задачки мы постарались сделать нескучными.

Коллекция сайтов постоянно пополняется: этим каждый день занимаются наши роботы, а помогают им родители и сами ребята — ведь никто, кроме них, не сможет сказать лучше, какие игры, истории или мультики нравятся им больше всего.»

Директор поисковой системы "Спутник", Максим Хромов 06.11.2014 рассказал ИТАР-ТАСС о проекте "Спутник.Дети". «Это будет поисковый сервис специально для детей. Область поиска составит коллекция сайтов, зарегистрированных в доменной зоне .Дети, а также детские сайты, найденные в Рунете автоматическими поисковыми роботами и анализаторами "Спутника", и сайты, отобранные партнерами проекта.

Принять участие в развитии сервиса может любой владелец интернет-проекта для детей - достаточно предложить свой сайт на добавление в область поиска. Каждый ресурс проходит проверку асессорами поисковика и системой безопасности.

Сегодня в Рунете довольно серьезный дефицит качественных детских ресурсов - на них невелик спрос, потому что он формируется родителями и требует активной позиции, постоянного исследования вопроса, поиска новых сервисов и контента для ребенка.

В мае 2015 года на Большом Медиа-Коммуникационном Форуме, Денис Жилин (фонд "Разумный Интернет") в своем докладе сообщил, что под категорию "Дети и семья" (т.е. сайты, содержащие детский контент) в России подпадают всего 64 000 сайтов (это чуть больше одного процента от всего Рунета). К ядру наиболее посещаемых из них относятся 5 000 сайтов.

Быть хорошим родителем непросто в принципе, а в эпоху интернета еще сложнее: необходимо постоянно повышать свою квалификацию. Или пустить все на самотек в формате "ребенок чем-то занят в планшете - значит при деле". Наша задача повысить доступность качественного развивающего контента, а вместе с тем обозначить безопасную орбиту, внутри которой ребенок будет в безопасности», - объяснил Максим Хромов.

Директор "Спутника" считает, что мобильные устройства не мешают развитию детей. Более того, неправильно в мире современных технологий и гаджетов воспитывать ребенка в изоляции от них: в определенный момент он рискует оказаться отстающим. Все зависит от подхода к этому вопросу.

На вопрос: Как Вы считаете, кого на сегодняшний момент надо обучать правилам пользования интернетом - детей или сначала их родителей?

Максим Хромов ответил: « - Марк Твен, кажется, говорил: "Не воспитывайте детей, все равно они будут похожи на вас. Воспитывайте себя". Этой фразе больше ста лет, но, мне кажется, сейчас она не менее актуальна. Если взрослый человек не знает, как правильно пользоваться компьютером, интернетом, как он сможет помочь своему ребенку разобраться в том, какой контент вреден, а какой нет?

В определенный момент развития общества нормальной была ситуация, когда компьютер и интернет в семье появлялись только для ребенка, а родители не знали даже, как все это включается. Сегодня ситуация меняется. Только в семье и школе ребенок может получить представление о том, что такое хорошо, и что такое плохо в интернете, именно поэтому соответствующее представление о предмете должны быть в первую очередь у родителей и учителей.»

Следует специально подчеркнуть, что в связи с постоянным ростом детской и подростковой аудитории сети Интернет, все большую актуальность приобретает проблема обеспечения информационно-психологической безопасности детей и подростков, общающихся в сети Интернет и социальных Интернет-сетях.

Для более точного понимания и системного изложения угроз информационно-психологической безопасности личности (ИПБ), следует рассмотреть определения данного понятия.

Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" определяет информационную безопасность детей как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [8].

В настоящее время нет единого подхода к определению понятия информационно-психологической безопасности. Исследователи данного вопроса выделяют собственные подходы к трактовке понятия ИПБ в соответствии с целями своего исследования. Так, на ранних этапах можно выделить подход к определению информационно-психологической безопасности как социокультурного феномена, как состояния общественного сознания, выделение информационно-психологической безопасности среды, психофизической безопасности. Позднее стали выделять информационно- психологическую безопасность личности как состояние защищенности личности и целостное личностное образование, также исследователи стали рассматривать психологическую безопасность с точки зрения безопасности среды (образовательной, трудовой, воспитательной), выделять психолого-экологическую безопасность, обеспечиваемой за счет нравственно-экологического сознания, рассматривать социально-психологическую безопасность как состояние защищенности личности в обществе.

В целом, информационно-психологическая безопасность личности может быть определена как интегративное объединение, отражающее:

1)психологическую защищенность личности от негативных воздействий информационных факторов и психологического насилия, посредством информационных технологий, при которой обеспечивается защита психологического здоровья личности и удовлетворены базовые потребности личности в самосохранении;

2)психологическую суверенность личности, целостность, обеспечивающее возможности осознанного саморазвития.

В соответствии с данным определением, угрозы информационно-психологической безопасности будут непосредственно воздействовать или на состояние защищенности личности или подрывать целостное личностное образование.

В таблице приведены основные угрозы информационно-психологической безопасности детей в сети Интернет.

Таблица

Угрозы информационно-психологической безопасности детей в сети Интернет

Компоненты ИПБ	Целостность личности	Защищенность личности
Угрозы ИПБ	Интернет-зависимость	Кибербуллинг
	Виртуализация личности	«Опасные» материалы
		Группы девиантного поведения, секты

	Эмоциональные и поведенческие нарушения	Сексуальные домогательства

Таким образом, угрозы информационно-психологической безопасности воздействуют или на целостность личности, или на состояние защищенности личности. По-сути это внутренние и внешние угрозы ИПБ в том значении, в котором их употреблял Г. В. Грачев [2]. Группа внутренних угроз, по нашему мнению, так же может быть названа «психологическими».

Группа внешних угроз представляет такие проблемы как группы девиантного поведения, «опасные» материалы, кибербуллинг, сексуальные домогательства. Данные угрозы могут быть нивелированы путем законодательного регулирования, родительского контроля, применения специальных программ ограничения доступа, но не всегда. Например, взаимодействие в современных Интернет-сетях зачастую позволяет злоумышленникам преодолевать данные ограничения.

1)**Группы девиантного поведения**

В сети Интернет существуют определенные группы, сети людей, объединенных определенной идеей девиантного поведения, часто носящие подчеркнуто негативный характер. Группа единомышленников стремится всячески расширять собственный состав участников, в том числе и за счет привлечения новых членов. В данном случае, подростковая аудитория является зачастую ключевой аудиторией подобных сообществ.

С. К. Тамазян классифицировала сетевые социальные организации подростков по своему назначению и роли на социально-негативные, социально-позитивные и социально-нейтральные.

К социально-негативным неформальным подростковым организациям, имеющим сетевую структуру, относятся сообщества спортивных фанатов, религиозно-ориентированные сообщества, прежде всего, языческого и сатанистского направлений, а также некоторые национально-патриотические сообщества. К социально-позитивным относятся неформальные объединения экологов и стрэйтэйджеров. Социально-нейтральными автор называет сетевые сообщества ролевиков, сторонников различных музыкальных течений и альтернативной культуры [7, с. 6-8].

2)**«Опасные» материалы**.

Под определение проблематичного или «опасного» контента подпадают разнообразные материалы, но большинство исследователей фокусируются на тех, которые содержат сцены насилия (фильмы, музыка, изображения) и порнографию. В этой связи упоминаются агрессивные высказывания, комментарии, выражения ненависти, детская порнография, а также контент, который может быть определен как оскорбительный. К данной группе угроз также можно отнести проявления эксгибиционизма в сети.

«Опасный» контент является причиной следующих проблем:

1) дети невольно сталкиваются с подобными материалами во время вполне «безобидных» сессий в интернете;

2) юные пользователи часто вполне компетентны для того, чтобы найти и получить доступ к запрещенному (родителями или законом) контенту;

3) произвольный или непроизвольный просмотр подобных материалов негативно сказывается на детской психике, поведении [1].

3)**Сексуальные домогательства с**вязаны с нежелательными контактами со злоумышленниками на почве сексуальных домогательств.

Исследования, проведенные в США, показывают, что чаще всего сексуальные домогательства в Сети исходят от ровесников детей (48%) или молодых взрослых в возрасте от 18 до 30 лет (30%), угрозы, исходящие от более взрослых пользователей (или от тех, чей возраст неизвестен), относительно малочисленны (4–9%) [9]. Не всегда угроза исходит от незнакомцев, 14% преследователей – это друзья, знакомые из реальной жизни детей [11] .

4)**Кибербуллинг** – это издевательства, унижения, разоблачения, оскорбления, агрессивные нападки, преследования посредством Интернет-технологий.

Исследование "Дети России онлайн", осуществленноесотрудниками Фонда Развития Интернет, факультета психологии МГУ им. М.В. Ломоносова и Федерального института развития образования Минобрнауки России, показывает, что основной площадкой кибербуллинга являются социальные сети. В них нередки случаи оскорбления человека в сообщениях, размещения унизительного контента через взламывание страницы жертвы или создания поддельной на ее имя. Особенно тяжело переживают кибербуллинг пользователи 9–10-ти лет: 52% детей этого возраста, сталкивались с кибербуллингом, в первую очередь девочки; 25% детей признались, что за последний год обижали или оскорбляли других людей в реальной жизни или в Интернете. Обращает на себя внимание тот факт, что в России субъектов буллинга в два раза больше, чем в среднем по европейским странам [6].

Вторая группа угроз информационно-психологической безопасности содержит внутренние угрозы: Интернет-зависимость, виртуализация личности, эмоциональные и поведенческие нарушения. Данный тип угроз действует на психологическом уровне, сложно поддается выявлению, медленно развивается и провоцирует нарушения детской психики и поведения.

1) **Интернет-зависимость**

В настоящее время явление Интернет-зависимости активно сейчас изучается в психологической науке (Наумова Т. А., Дрепа М. И., Ф. А. Саглам, В. А. Лоскутова, О. В. Завалишина).

В первую очередь, Интернет-зависимость может быть определена как форма технологической зависимости, выражающаяся в стремлении к уходу от реальности посредством изменения своего психического состояния фиксацией внимания на Интернет-ресурсах, в ослаблении возможности самостоятельного контроля времени, проводимого в Сети.

В. А. Лоскутова выделяет 3 группы проявления Интернет-зависимости: Первая группа — это психологические проявления, в которую входят позитивные чувства и эйфория, испытываемая в процессе общения в сети, невозможность остановиться, проблемы с семьей и друзьями и т. д. Вторая группа — это физические проявления, в которую входят синдром карпального канала, сухость в глазах, боли в спине и т. д. Третья группа — это поведенческие проявления, в которую входят тяга к поиску в сети,

навязчивое желание выйти в интернет и т. д. При этом, Интернет-зависимость проявляется при совокупности перечисленных признаков [4].

2)**Виртуализация личности** может быть рассмотрена в двух плоскостях:

1)создание виртуальной личности в сети Интернет и в социальной сети.

Здесь важно рассмотреть суть понятий «реальная» и «виртуальная» личность. Реальные личности – это пользователи, которые выходят в Интернет под своим именем и сетевая активность которых коррелирует с реальной жизнью. Причиной выхода в Интернет в качестве реальной личности может быть социальная ригидность, самодостаточность. Виртуальные личности именуются псевдонимами, а их биография в Интернете является вымышленной. Интенцией к созданию виртуальной личности может служить неудовлетворенность реальной жизнью, пресыщенность реальной жизнью, желание получить новые ощущения, потребность в конструировании иной – символической реальности для творческого самовыражения [5, с. 104].

2)подмена реального бытия в человеческом обществе виртуальным бытием в сети Интернет – ресоциализация личности, что ведет к социальному отчуждению и искусственной «аутизации» личности [3, с. 14-15]. Очевидно, что происходит виртуализации сознания, а соответственно игнорирование или виртуализация ответственности, принятия иных законов и норм отношений.

3) **Эмоциональные и поведенческие нарушения** приводят к:

- смене настроения и поведения ребенка после сеанса в Сети;

- перегруженности информацией;

эмоциональной холодности;

- эмоциональной нестабильности.

Итак, в настоящее время актуальной является проблема обеспечения информационно-психологической безопасности детей и подростков, общающихся в сети Интернет и социальных Интернет-сетях. Угрозы информационно-психологической безопасности непосредственно воздействуют или на состояние защищенности личности (кибербуллинг, «опасные» материалы, сексуальные домогательства, группы девиантного поведения в сети) или подрывают целостное личностное образование (Интернет-зависимость, виртуализация личности, эмоциональные и поведенческие нарушения).

Между тем, анализ проблемы обеспечения информационно-психологической безопасности детей в сети Интернет позволил выделить следующие проблемные вопросы в современном обществе:

1. Недостаточное внимание родителей к проблеме обеспечения информационно-психологической безопасности своих детей.

В ходе совместного исследования с Нижегородской региональной благотворительной общественной организацией «Забота» и Региональным Центром безопасного интернета для детей в рамках проекта «Погремушка, iPad и безопасный Интернет» было изучено отношение родителей к проблеме сетевой безопасности детей-дошкольников. Респондентам (родители детей 3-7 лет, посещающих детский сад) предлагалось ответить на вопросы, касательно применения их детьми сети Интернет и безопасности в Сети. Исследование проходило на базе детского сада № 389 (ОКБМ) г.

Нижнего Новгорода в июне-октябре 2012 года. В исследовании приняли участие 55 респондентов.

По результатам проведенного исследования был сделан вывод, что культура сетевой безопасности детей в России пока недостаточно сформирована. Практически все родители отмечают, что действительно Интернет представляет собой потенциальные угрозы для психологической безопасности детей, многие родители называют риски сети Интернет. Но при этом большая часть родителей не считает необходимым каким-либо специальным образом обучать детей безопасному использованию Интернет. Многие считают, что «еще рано думать на это тему», «ребенок еще маленький и не пользуется Интернетом». Наиболее эффективными приемами защиты ребенка в сети Интернет считают родительский контроль и специальные программы ограничения доступа, не уделяя должного внимания необходимости обучения ребенка безопасному использованию сети интернет, общению с ребенком на тему Интернета.

2.Недостаток программ обучения для педагогов в детских садах и школах. Безусловно, необходимы программы дополнительного профессионального образования (повышения квалификации), такие как, например, программа Академии повышения квалификации и профессиональной переподготовки работников образования «Здоровье и безопасность детей в мире компьютерных технологий и Интернет».

3. Недостаток программ психологической профилактики, психологической помощи при травмах, полученных в Сети, в том числе готовых программ для использования психологами в детских садах и школах.

Таким образом, для предупреждения рисков информационно-психологической безопасности подростков в сети Интернет необходимо широкое обсуждение проблемы Онлайн-безопасности детей и подростков в Сети, продолжение научных исследований по проблеме, разработка и внедрение программ по формированию навыков безопасного поведения в Сети для школьников и разработка программ психологической коррекции нарушений в личностной сфере подростков, пользующихся сетью Интернет.

ЛИТЕРАТУРА

1. *Годик Ю.О.* Угрозы и риски безопасности детской и подростковой аудитории новых медиа // Медиаскоп. 2011. № 2. URL: http://www.mediascope.ru/node/841
2. *Грачев Г.В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М., 1998.
3. *Завалишина О.В.* Педагогическая поддержка подростков, склонных к интернет-зависимости: Автореф. дис.… канд. пед. наук. Курск, 2012.
4. *Лоскутова В.А.* Интернет-зависимость как форма нехимических аддиктивных расстройств: Дис…. канд. мед. наук. Новосибирск, 2004
5. *Силаева В.Л.* Интернет как социальный феномен // Социс. 2008. № 11.
6. *Солдатова Г.В., Зотова Е.Д.* Опасности, подстерегающие ребенка в сети Интернет // Справочник классного руководителя. 2011. № 7.
7. *Тамазян С.К.* Сети социального взаимодействия подростков с девиантным поведением: Автореф.… канд. соц. наук. Ставрополь, 2011.

8. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" // "Российская газета". 31.12.2010. Федеральный выпуск № 5376.

9. *Finkelhor D.* Online Victimazation: A report on the Nation's Youth, 2000. URL: http://www.unh.edu/ccrc/trends/index.html

10. *Palfrey J., Gasser Urs.* Born Digital. Understanding the first generation of digital natives. N.Y., 2008.

ПАМЯТКА по безопасности детей в сети Интернет

Классификация интернет-угроз

Во Всемирной паутине существует следующие виды опасности юных пользователей:
- суицид-сайты;
- сайты-форумы потенциальных самоубийц;
- наркосайты (интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья»);
- сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
- сайты порнографической направленности;
- сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);
- сайты, пропагандирующих экстремизм, насилие и девиантные формы поведения, прямые угрозы жизни и здоровью школьников от незнакомцев, предлагающих личные встречи, а также различные виды мошенничества;
- секты (виртуальный собеседник может повлиять на мировоззрение подростка).

Правила работы в сети Интернет

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)
7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. Не всей информации, которая размещена в Интернете, можно верить.

10. Не оставляйте без присмотра компьютер с важными сведениям на экране
11. Не сохраняйте важные сведения на общедоступном компьютере.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интеренета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Wmdows\Temporary Internet Files в операционной системе Windows Vista). В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернет, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
• Используйте специальные детские поисковые машины, типа MSN Kids Search.
• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
• Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.
• Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
• Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
• Научите детей не загружать файлы, программы или музыку без вашего согласия.
• Не разрешайте детям использовать службы мгновенного обмена сообщениями.
• В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
• Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

• Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
• Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
• Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
• Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
• Не забывайте беседовать с детьми об их друзьях в Интернет.
• Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
• Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
• Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
• Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
• Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают

общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет. В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

• Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).
• Компьютер с подключением к сети Интернет должен находиться в общей комнате.
• Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
• Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
• Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.
• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
• Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
• Приучите себя знакомиться с сайтами, которые посещают подростки.
• Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
• Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Список терминов

• Аккаунт (англ.- account) - учетная запись, регистрационная запись.
• Антивирус — пакет компьютерных программ, останавливающий проникновение вирусов на ваш компьютер, осматривающий содержимое компьютера на предмет наличия вирусов. Антивирус также лечит и удаляет
• Администраторы, модераторы сайта — специальные сотрудники сайта, которые следят за исполнением установленных на сайте правил.
• Базы данных (БД) - специальное программное обеспечение, предназначенное для организации хранения и доступа к данным (информации). Используются при создании программных решений для автоматизации сайта.
• Браузер — программа, позволяющая просматривать страницы в сети Интернет. Самые популярные Opera, Mozilla Firefox, Google Chrome, Internet Explorer.
• Веб-сайт (англ. Website, от web — паутина и site — «место») в компьютерной сети. Когда говорят «своя страничка в Интернет», то подразумевается целый веб-сайт или личная страница в составе чужого сайта. Кроме веб-сайтов в сети Интернет так же доступны WAP-сайты для мобильных телефонов.
• Виртуальный собеседник (англ. chatterbot) — это компьютерная программа, которая создана для имитации речевого поведения человека при общении с одним или несколькими пользователями.
• Всемирная паутина – это все веб-сайты Интернета
• Домен (англ. domain), Доменный адрес (англ. domain name) - Область пространства иерархических имен сети Интернет, которая обозначается уникальным доменным именем, обслуживается набором серверов доменных имен (DNS) Для каждого зарегистрированного доменного имени определен единственный Администратор. Это более практичный аналог IP-адреса. Доменная адресация возникла в Интернет для удобства пользователей: легче запомнить доменный адрес (например, www.microsoft.com), чем четыре числа IP-адреса. Доменный адрес может содержать латинские буквы, цифры, точки и некоторые другие знаки.
• Доменный почтовый ящик, в который поступает почта, приходящая на любые возможные адреса домена (все-что-угодно@ваш-домен).
• Интерне́т (англ. Internet, МФА: [ˈɪn.tə.net][1]) — всемирная система объединённых компьютерных сетей для хранения и передачи информации.
• Игнор — игнорирование, занесение в черный список.
• Логин (от английского log in — «входить в») — это имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.
• Новые СМИ или новые медиа (англ. New media) — термин, который в конце XX века стали применять для интерактивных электронных изданий и новых форм коммуникации производителей контента с потребителями для обозначения отличий от традиционных медиа, таких как газеты, то есть этим термином обозначают процесс развития цифровых, сетевых технологий и коммуникаций.документов частного лица или организации.
• Он-лайн игры —игровой процесс основан на взаимодействии с другими игроками и игровым миром, требующий постоянного подключения к Интернету.
• Интернет-магазин Действующим Законодательством РФ не определено понятие «Интернет-магазин». В классическом понимании "Интернет-магазин"("Электронный магазин";, "Сетевой магазин"; и т.д.), - это интерактивный сайт, в котором: рекламируются товары и услуги, принимаются заказы на товары и услуги, посетителю,

предлагаются различные варианта оплаты заказанных товаров и услуг, возможна их мгновенная оплата через Интернет.
• Пароль — набор символов, известный только одному пользователю, необходимый для авторизации (для «входа») на сайте.
• Персональная страница (персональный сайт) - совокупность Web-страниц, с содержанием, описывающим сферу интересов какого-либо человека (группы лиц), обычно созданная им самим. Часто размещается на сервере бесплатного хостинга.
• Посетители - количество уникальных посетителей побывавших на страницах вашего ресурса.
• Почтовый ящик - дисковое пространство на почтовом сервере, выделенное для хранения, отправки писем пользователя и т.д. (приходящих на его адрес и подлежащих отправке).
• Псевдонимы (алиасы) - доменные имена, которые указывают на один и тот же web-проект.
• Размер дискового пространства - суммарный размер всей информации, хранимой на сервере провайдера в мегабайтах (Мб). Обычно в него включаются также размеры файлы журнала обращений (Log Files), почтовых ящиков и баз данных.
• Регистратор домена - юридическое лицо,оказывающее услуги по регистрации доменных имен и обеспечивающее передачу в Реестр.
Регистрация домена (доменного имени) - 1) Внесение имени и соответствующего ему IP-адреса в базу данных DNS-сервера. Регистрация в доменах верхнего уровня обычно платная. Регистрация доменов нижнего уровня обычно бесплатна и выполняется провайдером. 2) Закрепление определенного доменного имени за физическим или юридическим лицом, путем внесения соответствующей информации в регистрационную базу данных организации, координирующей распределение доменных имен.
• Родительский контроль — это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств — обеспечить безопасность ребенка в Интернете, и эти инструменты иногда называют семейными настройками и настройками семейной безопасности. Windows 7, Windows Vista, Xbox 360, Xbox Live, Bing и другие продукты Microsoft включают встроенные настройки семейной безопасности
• Сайт (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») — совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).
• Сервер (Web-сервер) -1) Компьютер или специализированное устройство в сети со специальным программным обеспечением, обеспечивающий доступ многих пользователей к расположенной на нем информации и функционирование любых необходимых сервисов Интернет: http (сайт), E-mail (электронная почта), конференции, ftp и т.п. Для размещения сайта в Интернет необходим веб-сервер с поддержкой как минимум сервиса http. 2) Сайт, крупный информационный ресурс Интернета.
• Спам (англ. spam) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Незапрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM (англ.)русск. (англ. Spam over IM).
• Социальные сети — сайты в Интернете, на которых рядовые пользователи заводят

свои странички для общения с друзьями. Одна из обычных черт социальных сетей — система «друзей» и «групп». Самые популярные русскоязычные: ВКонтакте, Одноклассники.ш, Мой Мир, Мой Круг, ЖЖ и др.
• Трафик (traffic) - поток (объем) информации, проходящей через канал связи, приходящийся на сайт. Может быть исходящим и входящим.
• Тролли, троллинг — (от англ. trolling — «ловля на блесну») — размещение в Интернете провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления и т. п.
• Файлы, скачивание. Вся информация в компьютере сохраняется в виде файлов. Это могут быть текстовые файлы, музыкальные, видео, графические, мультимедийные и проч. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, скачивать, то есть сохранять на свой компьютер.
• Фишинг (от английского fish — «ловить рыбу»)- вид мошенничества в интернете, когда у пользователя пытаются узнать логины и пароли.
• «Черный список сайтов» (black list), или как еще его называют "скам лист". представляет собой список сайтов, проектов или людей, которые проводят мошеннические операции в сети или не выполняют взятые на себя обязательства. В такие "черные списки" (black list), никогда не помешает заглянуть человеку, прежде чем начать с кем-то сотрудничать или пользоваться каким-либо сервисом.
• Хиты - количество просмотров страниц, на которых побывали посетители ресурса.
• Хостер (hoster) - Синоним слова хостинг-провайдер (см.)
• Хостинг (hosting) - Услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности. В большинстве случаев предоставляется виртуальный сервер (т.н. виртуальный хостинг), т.е. программное обеспечение, обеспечивающее работу необходимых Вам сервисов, но работающее на одной аппаратной платформе с другими подобными виртуальными серверами. Различают также платный (коммерческий) и бесплатный хостинг.
• Хостинг-провайдер (hosting provider) - организация, профессионально занимающаяся предоставлением услуг Хостинга. Лучше выбирать услуги профессиональных Хостеров, т.е. Компаний, основной деятельностью которых является Хостинг, а не обычных Интернет-провайдеров, для которых Хостинг дополнительная услуга к основной.
• Хосты - количество посетителей с уникальным IP-адресом.
• Электро́нная по́чта (англ. email, e-mail, от англ. electronic mail) — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, задержки передачи сообщений, достаточную надёжность и в то же время отсутствие гарантии доставки.

Ссылка на первоисточник: http://webcache.googleusercontent.com/search?q=cache:niCp9ji-d30J:s24002.edu35.ru/attachments/category/32/%25D0%259E%2520%25D0%25B1%25D0%25B5%25D0%25B7%25D0%25BE%25D0%25BF%25D0%25B0%25D1%2581%25D0%25BD%25D0%25BE%25D1%2581%25D1%2582%25D1%2582%25D0%25B8%2520%25D0%25B4%25D0%25B5%25D1%2582%25D0%25B5%25D0%25B9%2520%25D0%25B2%2520%25D1%2581%25D0%25B5%25D1%2582%25D0%25B8%2520%25D0%2598%25D0%25BD%25D1%

2582%25D0%25B5%25D1%2580%25D0%25BD%25D0%25B5%25D1%2582-%25D0%25BF%25D0%25B0%25D0%25BC%25D1%258F%25D1%2582%25D0%25BA%25D0%25B0-%25D1%2580%25D0%25BE%25D0%25B4%25D0%25B8%25D1%2582%25D0%25B5%25D0%25BB%25D0%25B8.doc+&cd=8&hl=ru&ct=clnk&gl=ru
Ссылка на первоисточник